る場合には、同項に規定する営業所の設置の届出が必要であることに留意する。

●III －３－６－３ 監督手法・対応

検査結果、不祥事件等届出書等により、事務リスクの管理態勢に問題があると認められる場合には、必要に応じ、法第24条に基づき報告を求め、重大な問題があると認められる場合には、法第26条に基づき業務改善命令を発出する等の対応を行うものとする。

III －３－７ システムリスク

●III －３－７－１ システムリスク

●III －３－７－１－１ 意義

システムリスクとは、コンピュータシステムのダウン又は誤作動等のシステムの不備等に伴い、顧客や銀行が損失を被るリスクやコンピュータが不正に使用されることにより顧客や銀行が損失を被るリスクをいうが、銀行の経営再編に伴うシステム統合や新商品・サービスの拡大等に伴い、銀行の情報システムは一段と高度化・複雑化し、さらにコンピュータのネットワーク化の拡大に伴い、重要情報に対する不正なアクセス、漏えい等のリスクが大きくなっている。

特に主要行等のシステムについては、元来、機能が高度である一方、大量処理が求められていることから、規模が大きく、構成が複雑である傾向にある。加えて、累次の経営再編によりシステム構成、システム運用体制が、一層複雑化していることから、特にシステム上の諸課題に的確に対応することが求められている。仮に主要行等において、システム障害やサイバーセキュリティ事案が発生した場合は、利用者の社会経済生活、企業等の経済活動、ひいては、我が国経済全体にも極めて大きな影響を及ぼすおそれがあるほか、その影響は単に一銀行の問題にとどまらず、金融システム全体に及びかねないことから、システムが安全かつ安定的に稼動することは決済システム及び銀行に対する信頼性を確保するための大前提であり、システムリスク管理態勢の充実強化は極めて重要である。

（注）サイバーセキュリティ事案とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃等の、いわゆる「サイバー攻撃」により、サイバーセキュリティが脅かされる事案をいう。

（参考）預金等受入金融機関に係る検査マニュアル

「システムリスク」とは、コンピュータシステムのダウン又は誤作動等、システムの不備等に伴い金融機関が損失を被るリスク、さらにコンピュータが不正に利用されることにより金融機関が損失を被るリスクをいう。

●III －３－７－１－２ 主な着眼点

(1) システムリスクに対する認識等

① システムリスクについて代表取締役をはじめ、役職員がその重要性を十分認識し、定期的なレビューを行うとともに、全行的なリスク管理の基本方針が策定されているか。

② 代表取締役は、システム障害やサイバーセキュリティ事案（以下「システム障害等」という。）の未然防止と発生時の迅速な復旧対応について、経営上の重大な課題と認識し、態勢を整備しているか。

③ 取締役会は、システムリスクの重要性を十分に認識した上で、システムに関する十分な知識・経験を有し業務を適切に遂行できる者を、システムを統括管理する役員として定めているか。

④ 代表取締役及び取締役（委員会設置会社にあっては執行役）は、システム障害等発生の危機時において、果たすべき責任やとるべき対応について具体的に定めているか。

また、自らが指揮を執る訓練を行い、その実効性を確保しているか。

(2) システムリスク管理態勢

① 取締役会は、コンピュータシステムのネットワーク化の進展等により、リスクが顕在化した場合、その影響が連鎖し、広域化・深刻化する傾向にあるなど、経営に重大な影響を与える可能性があるということを十分踏まえ、リスク管理態勢を整備しているか。

② システムリスク管理の基本方針が定められているか。システムリスク管理の基本方針には、セキュリティポリシー(組織の情報資産を適切に保護するための基本方針)及び外部委託先に関する方針が含まれているか。

③ システムリスク管理態勢の整備に当たっては、その内容について客観的な水準が判定できるものを根拠としているか。

また、システムリスク管理態勢は、システム障害等の把握・分析、リスク管理の実施結果や技術進展等に応じて、不断に見直しを実施しているか。

(3) システムリスク評価

① システムリスク管理部門は、顧客チャネルの多様化による大量取引の発生や、ネットワークの拡充によるシステム障害等の影響の複雑化・広範化など、外部環境の変化によりリスクが多様化していることを踏まえ、定期的に又は適時にリスクを認識・評価しているか。

また、洗い出したリスクに対し、十分な対応策を講じているか。

② システムリスク管理部門は、例えば1口座当たりの未記帳取引明細の保有可能件数などのシステムの制限値を把握・管理し、制限値を超えた場合のシステム面・事務面の対応策を検討しているか。

③ 商品開発の担当部門は、新商品の導入時又は商品内容の変更時に、システムリスク管理部門と連携するとともに、システムリスク管理部門は、システム開発の有無にかかわらず、関連するシステムの評価を実施しているか。

(4) 情報セキュリティ管理

① 情報資産を適切に管理するために方針の策定、組織体制の整備、社内規程の策定、内部管理態勢の整備を図っているか。また、他社における不正・不祥事件も参考に、情報セキュリティ管理態勢のPDCAサイクルによる継続的な改善を図っているか。

② 情報の機密性、完全性、可用性を維持するために、情報セキュリティに係る管理者を定め、その役割・責任を明確にした上で、管理しているか。また、管理者は、システム、データ、ネットワーク管理上のセキュリティに関することについて統括しているか。

③ コンピュータシステムの不正使用防止対策、不正アクセス防止対策、コンピュータウィルス等の不正プログラムの侵入防止対策等を実施しているか。

④ 金融機関が責任を負うべき顧客の重要情報を網羅的に洗い出し、把握、管理しているか。

顧客の重要情報の洗い出しにあたっては、業務、システム、外部委託先を対象範囲とし、例えば、以下のようなデータを洗い出しの対象範囲としているか。

- 通常の業務では使用しないシステム領域に格納されたデータ
- 障害解析のためにシステムから出力された障害解析用データ
- ATM(店舗外含む)等に保存されている取引ログ　等

⑤ 洗い出した顧客の重要情報について、重要度判定やリスク評価を実施しているか。

また、それぞれの重要度やリスクに応じ、以下のような情報管理ルールを策定しているか。

- 情報の暗号化、マスキングのルール
- 情報を利用する際の利用ルール
- 記録媒体等の取扱いルール　等

⑥　顧客の重要情報について、以下のような不正アクセス、不正情報取得、情報漏えい等を牽制、防止する仕組みを導入しているか。

- 職員の権限に応じて必要な範囲に限定されたアクセス権限の付与
- アクセス記録の保存、検証
- 開発担当者と運用担当者の分離、管理者と担当者の分離等の相互牽制体制等

⑦　機密情報について、暗号化やマスキング等の管理ルールを定めているか。また、暗号化プログラム、暗号鍵、暗号化プログラムの設計書等の管理に関するルールを定めているか。

なお、「機密情報」とは、暗証番号、パスワード、クレジットカード情報等、顧客に損失が発生する可能性のある情報をいう。

⑧　機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。

⑨　情報資産について、管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢を継続的に見直しているか。

⑩　セキュリティ意識の向上を図るため、全役職員に対するセキュリティ教育（外部委託先におけるセキュリティ教育を含む）を行っているか。

(5)　サイバーセキュリティ管理

①　サイバーセキュリティについて、取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。

②　サイバーセキュリティについて、組織体制の整備、社内規程の策定のほか、以下のようなサイバーセキュリティ管理態勢の整備を図っているか。

- サイバー攻撃に対する監視体制
- サイバー攻撃を受けた際の報告及び広報体制
- 組織内CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制
- 情報共有機関等を通じた情報収集・共有体制　等

③　サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。

- 入口対策（例えば、ファイアウォールの設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入　等）
- 内部対策（例えば、特権ID・パスワードの適切な管理、不要なIDの削除、特定コマンドの実行監視　等）
- 出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断　等）

④　サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。

- 攻撃元のIPアドレスの特定と遮断
- DDoS攻撃に対して自動的にアクセスを分散させる機能
- システムの全部又は一部の一時的停止　等

⑤　システムの脆弱性について、OSの最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。

⑥　サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、セキュリティ対策の向上を図っているか。

⑦　インターネット等の通信手段を利用した非対面の取引を行う場合には、Ⅲ−３−８−２（２）によるセキュリティの確保を講じているか。認証方式や不正防止策として、全国銀行協会の申し合わせ等には、以下のようなセキュリティ対策事例が記載されている。

- 可変式パスワードや電子証明書などの、固定式のID・パスワードのみに頼らない認証方式
- 取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証
- ハードウェアトークン等でトランザクション署名を行うトランザクション認証
- 取引時においてウィルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供
- 利用者のパソコンのウィルス感染状況を金融機関側で検知し、警告を発するソフトの導入
- 電子証明書をIC カード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用
- 不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備　等

⑧　サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。

⑨　サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。

(6)　システム企画・開発・運用管理

①　経営戦略の一環としてシステム戦略方針を明確にした上で、中長期の開発計画を策定しているか。

　また、中長期の開発計画は、取締役会の承認を受けているか。

②　現行システムに内在するリスクを継続的に洗い出し、その維持・改善のための投資を計画的に行っているか。

③　開発案件の企画・開発・移行の承認ルールが明確になっているか。

④　開発プロジェクトごとに責任者を定め、開発計画に基づき進捗管理されているか。

⑤　システム開発に当たっては、テスト計画を作成し、ユーザー部門も参加するなど、適切かつ十分にテストを行っているか。

⑥　人材育成については、現行システムの仕組み及び開発技術の継承並びに専門性を持った人材の育成のための具体的な計画を策定し、実施しているか。

(7)　システム監査

①　システム部門から独立した内部監査部門が、定期的にシステム監査を行っているか。

②　システム関係に精通した要員による内部監査や、システム監査人等による外部監査の活用を行っているか。

③　監査対象は、システムリスクに関する業務全体をカバーしているか。

関係する海外監督当局との連携を検討する。

(2) その際、関係する海外監督当局との情報交換等を通じて、海外営業拠点の業務運営状況を確認するとともに、問題認識の共有を図り、必要に応じて、法第24条に基づき報告を求め、重大な問題があると認められる場合には、法第26条に基づく業務改善命令を発出する等の対応を行うものとする。

金融庁/Financial Services Agency, The Japanese Government
Copyright(C) 2016 金融庁 All Rights Reserved.